SD-WAN et SASE : Révolution de la connectivité et renforcement révolutionnaire de la sécurité

1ère CHERIFI Sarah
Département de Génie Électrique et Informatique Industrielle
École Nationale Supérieure de Technologie
Alger, Algérie
s_cherifi@enst.dz

2ème HARCHAD Ranya
Département de Génie Électrique et Informatique Industrielle
École Nationale Supérieure de Technologie
Alger, Algérie
r_harchad@enst.dz

3ème BENDOUDA Djamila
Département de Génie Électrique et Informatique Industrielle
École Nationale Supérieure de Technologie
Alger, Algérie
djamila.bendouda@enst.dz

***Abstract*—L'émergence du réseau étendu défini par logiciel (SD-WAN) a révolutionné la connectivité des réseaux d'entreprise grâce à son infrastructure intelligente, rentable et évolutive. Cependant, l'escalade des menaces en matière de cybersécurité a contraint les entreprises à rechercher des solutions pour protéger leur infrastructure réseau contre les cyberattaques. La technologie Secure Access Service Edge (SASE) a été développée pour répondre à ce besoin en combinant la connectivité WAN avec une sécurité basée sur le cloud en tant que service. Cette approche intégrée permet une protection plus efficace et une réduction des coûts en unifiant le réseau et la sécurité dans une seule solution. Dans ce contexte, cette étude se concentre sur l'intégration de SASE dans SD-WAN. L'objectif est d'analyser comment cette technologie peut avoir un impact significatif sur la sécurité et les performances du réseau pour les entreprises. Cette étude vise à discuter des considérations clés et à présenter une analyse approfondie pour illustrer les améliorations de la connectivité et le renforcement de la sécurité obtenus grâce à l'implémentation combinée de SD-WAN et de SASE.**

***Index Terms*—SD-WAN, SASE, WAN, NetOps, SecOps, IPS, IDS, HTTPS/TLS, AMP, DNS, URLF, MPLS, SDN, Cloud.**

I. Introduction

Le paysage numérique évolue constamment, et les organisations reconnaissent de plus en plus l'importance d'établir une connectivité réseau sécurisée et fiable. En réponse à cette demande, le concept de SASE a émergé en tant qu'approche transformative. Dans cet article, intitulé "SD-WAN et SASE : Révolution de la connectivité et renforcement révolutionnaire de la sécurité", nous explorons l'intégration du SD-WAN et de SASE, ainsi que ses implications pour renforcer la sécurité et la connectivité dans les architectures de réseau modernes.

Les infrastructures réseau traditionnelles ne parviennent souvent pas à répondre aux exigences de l'environnement commercial dynamique d'aujourd'hui, où les organisations ont besoin d'une solution globale qui optimise les performances du réseau tout en garantissant des mesures de sécurité robustes [1]. SASE fournit un cadre unifié qui combine la connectivité réseau et les services de sécurité, en les fournissant depuis le cloud.

Nous approfondissons les principes fondamentaux de SD-WAN, mettant en évidence sa capacité à optimiser les performances du réseau, à améliorer l'agilité et à rationaliser les processus de gestion dans des sites géographiquement dispersés. Nous explorons également les concepts et les principales caractéristiques de SASE, en mettant l'accent sur son approche intégrée pour fournir une connectivité réseau sécurisée et des services de sécurité avancés [2]. Cisco SD-WAN joue un rôle primordial dans l'intégration de SD-WAN et de SASE, en exploitant ses capacités telles que l'optimisation du trafic et la gestion centralisée pour permettre une connectivité améliorée et une efficacité réseau [3].

Alors que les organisations se lancent dans leur parcours vers l'architecture SASE, ce guide explore les fonctionnalités de sécurité intégrées de SD-WAN. Nous abordons les mesures de sécurité du tissu, notamment la confiance basée sur le matériel, la liste blanche, la vérification de l'identité des contrôleurs et des routeurs de bord, ainsi que les plans de contrôle et de données sécurisés. De plus, nous explorons les fonctionnalités de sécurité intégrées de SASE, telles que les pare-feu sensibles aux applications, les systèmes de prévention des intrusions IPS (Intrusion Prevention System), les mandataires HTTPS/TLS (Hypertext Transfer Protocol Secure/Transport Layer Security), le filtrage d'URL (Uniform Resource Locator), la protection avancée contre les logiciels malveillants AMP (Advanced Malware Protection) et la sécurité web basée sur le système de noms de domaine DNS (Domain Name System) [5]. En intégrant SD-WAN et SASE, les organisations peuvent bénéficier d'une connectivité améliorée, d'une sécurité renforcée, d'une gestion simplifiée du réseau et de coûts opérationnels réduits.

L'objectif est de fournir des informations précieuses sur l'intégration de ces technologies, permettant aux organisations d'établir une infrastructure réseau robuste et sécurisée répondant aux exigences évolutives de l'ère numérique. Dans les sections suivantes, nous approfondirons les principes de SD-WAN et ses aspects de sécurité, notamment la sécurité du tissu et les fonctionnalités de sécurité intégrées. Nous explorerons également les services de sécurité complets offerts par SASE, offrant une compréhension globale de la manière dont l'intégration de SD-WAN et de SASE améliore à la fois la sécurité et la connectivité dans les architectures de réseau modernes.

II. Réseau étendu défini par logiciel SD-WAN

Le SD-WAN est une technologie qui offre aux organisations un contrôle, une agilité et une efficacité accrue dans la gestion de leurs réseaux étendus. En utilisant les principes de la définition logicielle, le SD-WAN permet une gestion centralisée et un contrôle du trafic réseau [6]. Cela permet un acheminement dynamique et intelligent du trafic, optimisant la bande passante et garantissant une qualité de service optimale pour les applications critiques. En plus de l'optimisation, le SD-WAN simplifie les opérations réseau grâce à une gestion et une configuration centralisées, facilitant le déploiement rapide de nouveaux sites ou services. Il optimise également le trafic sur différentes connexions réseau, telles que le MPLS, l'Internet à large bande et les liens sans fil, offrant ainsi une connectivité fiable et sécurisée tout en utilisant des connexions Internet rentables. De plus, le SD-WAN intègre des fonctionnalités avancées de sécurité telles que le chiffrement, les pare-feu et la détection des menaces, assurant une connectivité sécurisée pour les sites distants et préservant la confidentialité et l'intégrité des données, tout en simplifiant le déploiement et la gestion des politiques de sécurité à l'échelle du réseau [7].

III. Principaux composants de SASE

Le SASE révolutionne les réseaux et la sécurité en les intégrant dans une solution unifiée. Il répond efficacement aux défis des architectures distribuées modernes et des effectifs distants [8]. Les composants clés du SASE, qui unifient les réseaux et la sécurité, comprennent la mise en réseau, la sécurité, un modèle de confiance zéro (Zero Trust security), les opérations réseau (NetOps) et les opérations de sécurité (SecOps).

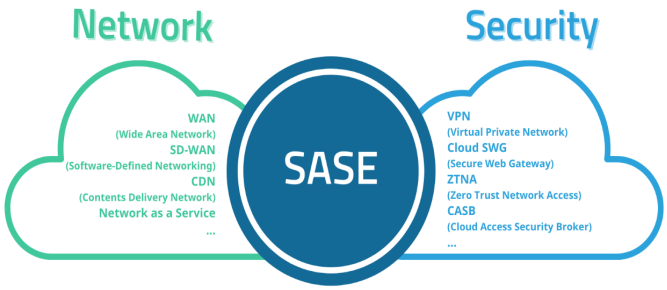


Fig. 1. Secure Access Service Edge (SASE) [9]

En termes de mise en réseau, le SASE utilise les principes de mise en réseau définis par logiciel (SDN), en particulier le SD-WAN, pour établir une connectivité réseau agile et optimisée, permettant des connexions sécurisées entre les succursales, les centres de données et les ressources cloud (Figure 1) [10]. L'aspect sécurité du SASE intègre une pile de sécurité complète, intégrant plusieurs fonctions telles que les passerelles web sécurisées, le pare-feu en tant que service, la prévention de la perte de données et le renseignement sur les menaces, garantissant une protection continue et performante pour tout le trafic [10]. Le SASE adopte un modèle de sécurité Zero Trust, mettant l'accent sur l'authentification approfondie, l'autorisation et la surveillance continue des demandes d'accès pour vérifier les utilisateurs et les appareils légitimes tout en prévenant l'accès non autorisé [4]. Les fonctionnalités NetOps surveillent et gèrent de manière optimale le réseau et les applications, en se concentrant sur les performances et l'optimisation du réseau, tandis que les capacités SecOps surveillent et gèrent les menaces, les vulnérabilités et la conformité réglementaire [11]. Ces composants clés se combinent pour offrir aux organisations une solution puissante pour gérer de manière sécurisée et de manière performante leurs réseaux étendus.

IV. Pourquoi avons-nous besoin de SASE ?

Dans le contexte dynamique du monde numérique d'aujourd'hui, les modèles traditionnels de sécurité et les approches en matière de mise en réseau ne parviennent pas à relever les défis auxquels les organisations sont confrontées. L'adoption de SASE revêt une importance capitale pour plusieurs raisons convaincantes: [2]

1) ***Adoption du cloud et architectures distribuées****:* SASE s'intègre harmonieusement aux ressources cloud et offre un accès sécurisé depuis n'importe quel endroit, ce qui en fait une solution idéale pour les environnements distribués.

2) ***Effectifs à distance et Appareils Mobiles****:* SASE permet aux organisations d'étendre en toute sécurité leur périmètre réseau aux travailleurs à distance et aux appareils mobiles, garantissant un accès sécurisé aux ressources de l'entreprise sans compromettre la sécurité.

3) ***Scalabilité et flexibilité****:* SASE offre aux organisations la possibilité d'étendre en toute sécurité leur périmètre réseau pour s'adapter aux travailleurs à distance et aux appareils mobiles, assurant ainsi un accès sécurisé aux ressources de l'entreprise sans compromettre la sécurité.

4) ***Gestion Simplifiée et Efficacité Coût****:* SASE simplifie la gestion du réseau et de la sécurité, réduisant la complexité et les coûts associés à la gestion de plusieurs solutions.

5) ***Protection accrue contre les menaces****:* Grâce à sa pile de sécurité intégrée, à une surveillance continue et aux principes de confiance zéro, SASE offre une protection avancée contre les menaces. Il permet aux organisations d'identifier et de prévenir proactivement les risques de sécurité, protégeant ainsi les données sensibles et prévenant les cyber-attaques potentielles.

V. Avantages de l'intégration de SD-WAN et SASE

L'intégration de SD-WAN et SASE offre des avantages significatifs en termes de connectivité, de performances et de sécurité. Ce cadre complet combine la sécurité du réseau, la sécurité intégrée et la sécurité cloud, renforçant l'infrastructure numérique de l'organisation et offrant une approche unifiée de la connectivité réseau et de la protection contre les menaces. Il simplifie la gestion des politiques de sécurité, garantit une protection cohérente et robuste, maintient l'intégrité des données et préserve la confidentialité des utilisateurs sur l'ensemble

du réseau étendu [3]. Le tableau fournit un aperçu concis de chaque composant, notamment la sécurité du tissu, la sécurité intégrée et la sécurité cloud. (Figure 2).

Sécurité du tissu	Sécurité intégrée	Sécurité Cloud
Sécurité Matérielle (SUDI)	FW d'entreprise	Umbrella
Modèle de Confiance Zéro (Whitelesting)	IPS	
Identité de l'appareil (Certificates)	URL Filtering	
Plan de contrôle sécurisé (DTLS/TLS)	AMP	
Plan de données chiffré (IP-Sec)	TLS Proxy	
	Identité FW	

Fig. 2. Aperçu de la sécurité

VI. Sécurité de Tissu

La sécurité du tissu (ou infrastructure) revêt une importance primordiale pour les organisations, afin d'assurer l'intégrité du réseau et se prémunir contre les menaces potentielles. Face à ce défi, il est essentiel de se demander comment établir la confiance dans les dispositifs réseau, sans se reposer uniquement sur les mécanismes de sécurité traditionnels. Dans cette section, nous allons explorer différentes approches qui permettent de répondre à cette préoccupation.

A. Confiance basée sur le matériel (SUDI)

La sécurisation des dispositifs réseau repose largement sur le SUDI (Secure Unique Device Identifier). Cisco utilise un module d'ancrage de confiance TAm(Trust Anchor Module) lors de la fabrication, incorporant plusieurs fonctionnalités de sécurité pour se protéger contre les menaces. Le démarrage sécurisé (Secure Boot) garantit un démarrage sécurisé du dispositif en surveillant le processus de démarrage et en empêchant l'infiltration de code malveillant. Le stockage sécurisé (Secure Storage) offre une zone protégée pour stocker les informations critiques du dispositif, y compris les clés de chiffrement, les mots de passe et les informations d'identification du client. L'identifiant de dispositif unique sécurisé (SUDI) valide l'authenticité du dispositif grâce à un certificat SSL(Secure Sockets Layer) qui contient le numéro de série du dispositif et l'identifiant du produit. SUDI obtient une validation auprès d'une autorité de certification racine publique, garantissant la confiance et l'authenticité. La défense en temps d'exécution , RTD(Runtime Defense) agit comme un mécanisme de défense proactif, protégeant contre la compromission du micrologiciel pendant l'exécution du dispositif. En mettant en œuvre ces mesures, Cisco assure l'intégrité et la sécurité du dispositif tout au long de son cycle de vie. [12]

B. Liste blanche de WAN Edge

Pour sécuriser le réseau SD-WAN, Il est impératif d'authentifier. et d'autoriser les appareils participants. Cisco utilise un modèle de liste d'autorisation, accordant une approbation explicite aux routeurs et aux contrôleurs de points de terminaison WAN pour rejoindre le réseau. La liste des points de terminaison WAN est générée à partir des numéros de série enregistrés des routeurs de WAN Edge achetés, qui sont enregistrés dans le portail Cisco Plug-and-Play (PnP). Ces numéros de série sont ensuite distribués à tous les contrôleurs SD-WAN via vManage. Par conséquent, les contrôleurs SD-WAN possèdent une liste d'autorisation complète des appareils autorisés, empêchant tout accès non autorisé aux plans de contrôle et de gestion centralisés. [13]

C. Vérification d'identité

Dans un réseau SD-WAN, Il est indispensable d'établir et de vérifier l'identité des appareils pour garantir un environnement réseau sécurisé. Cela implique l'utilisation de certificats SSL et d'un processus de validation. [14] Explorons les mécanismes d'identité et de vérification dans un SD-WAN (Figure 3).

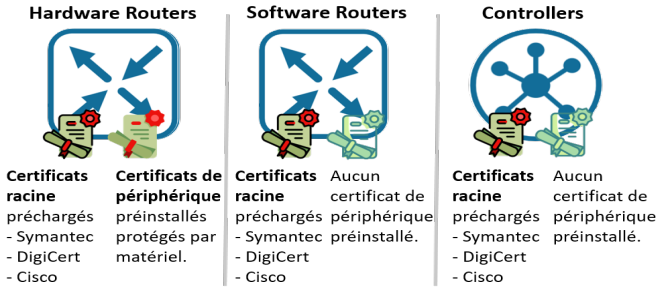


Fig. 3. Identité de l'appareil SD-WAN

*1) **Identité des appareils SD-WAN**:* Pour garantir l'authenticité des appareils SD-WAN, des certificats SSL (x509v3) sont utilisés. Des certificats racines préinstallés provenant d'autorités réputées telles que DigiCert, Symantec et Cisco sont intégrés à tous les appareils. Les routeurs physiques disposent d'une couche de sécurité supplémentaire avec un certificat d'appareil préchargé stocké dans une puce matérielle appelée SUDI. En revanche, les appareils basés sur des logiciels, y compris les routeurs et les contrôleurs cloud, doivent passer par un processus de demande de signature de certificat CSR(Certificate Signing Request) pour obtenir leurs certificats. [13]

*2) **Vérification de l'identité du contrôleur**:* Lorsque les contrôleurs établissent des connexions de contrôle, ils échangent des certificats SSL lors de la poignée de main (Datagram Transport Layer Security/Transport Layer Security) (DTLS/TLS). Pour garantir la validité de l'identité des contrôleurs, plusieurs vérifications sont effectuées : [13]

- Le certificat d'appareil reçu est validé par rapport aux certificats racines préinstallés pour établir la confiance.
- Le numéro de série du certificat est comparé à la liste des contrôleurs autorisés distribuée par vManage.
- Le champ du nom de l'organisation dans le certificat est comparé au nom de l'organisation configuré localement.

*3) **Vérification de l'identité du routeur Edge d'extrémité**:* Lors de l'établissement des connexions de contrôle entre les routeurs d'extrémité WAN Edge et les contrôleurs SD-WAN, les routeurs d'extrémité présentent leurs certificats SSL

d'appareil. Les contrôleurs vérifient l'identité des routeurs d'extrémité en utilisant le même ensemble de vérifications effectuées pour les contrôleurs.

En exploitant les certificats SSL et en mettant en œuvre des processus de vérification d'identité, SD-WAN renforce la sécurité globale du réseau. Ce cadre d'identité robuste atténue les risques liés à l'accès non autorisé et assure une communication sécurisée entre les appareils SD-WAN.

D. Plan de contrôle sécurisé

Le plan de contrôle sécurisé dans un SD-WAN garantit l'intégrité et l'authenticité des communications du plan de contrôle grâce à la mise en œuvre de mesures de sécurité clés. Il repose sur deux éléments essentiels : les condensés de message AES-GCM (Advanced Encryption Standard Galois/Counter Mode) et les clés publiques-privées. AES-GCM assure le chiffrement et la vérification d'intégrité des messages au sein des tunnels DTLS/TLS, tandis que les clés publiques-privées garantissent l'authenticité des paquets transmis par des appareils de confiance. En utilisant des connexions DTLS/TLS authentifiées et chiffrées, le plan de contrôle sécurisé adresse de manière adéquate les préoccupations de sécurité liées aux protocoles de réseau natifs tels que SNMP et NETCONF [13], comme illustré dans la figure 4.

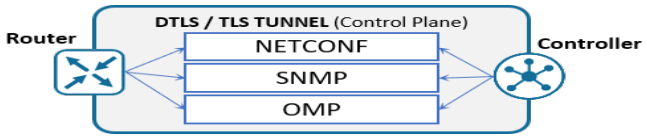


Fig. 4. Plan de contrôle sécurisé

E. Plan de données chiffré

Le plan de données chiffré, également appelé plan de transfert, joue un rôle essentiel dans SD-WAN en transférant de manière sécurisée le trafic utilisateur sur le réseau superposé via des tunnels IPsec. Il intègre trois composants de sécurité clés : l'authentification, le chiffrement et l'intégrité [14]. L'authentification dans le plan de données implique l'échange de clés de chiffrement IPsec (Internet Protocol Security) facilité par les contrôleurs vSmart. Le chiffrement des données est réalisé à l'aide de l'algorithme de chiffrement AES-GCM-256 robuste qui garantit que les données transmises restent confidentielles, protégées contre tout accès ou interception non autorisé.

Afin de maintenir l'intégrité des données en utilisant une encapsulation améliorée du protocole ESP(Encapsulating Security Payload), le mécanisme AH (Authentication Header) vérifie l'intégrité des en-têtes IP et UDP (User Datagram Protocol), tandis qu'un mécanisme anti-rejeu prévient les attaques de duplication de paquets. Cela renforce la sécurité du plan de données. [15]

VII. Sécurité intégrée

La sécurité intégrée fait référence à l'incorporation de différentes fonctions de sécurité, telles que le pare-feu, l'IPS et l'AMP, directement dans le micrologiciel des routeurs. Dans le contexte actuel de la sécurité, les organisations accordent une grande importance à la sécurité du réseau, et le pare-feu est considéré comme un composant vital. Une approche de sécurité avancée a été introduite en intégrant un pare-feu d'entreprise conscient des applications directement dans le micrologiciel des routeurs de périphérie, ce qui élimine le besoin de dispositifs matériels distincts [16]. Ce pare-feu intégré, connu sous le nom de Zone-Based Firewall (ZBFW), offre une flexibilité et une efficacité accrues par rapport aux architectures traditionnelles.

A. L'Architecture ZBFW

L'architecture du pare-feu ZBFW est une avancée significative dans la sécurité réseau, offrant une flexibilité améliorée et un meilleur contrôle de l'inspection du trafic. Elle remplace l'ancienne architecture du Contrôle d'accès basé sur le contexte (CBAC) et introduit le concept novateur de zones. Ces zones regroupent plusieurs interfaces de routeur et permettent la mise en œuvre de politiques de sécurité adaptées [17]. Les paires de zones jouent un rôle clé en établissant des associations logiques entre deux zones, ce qui permet aux administrateurs de définir des règles de sécurité spécifiques pour le trafic circulant entre ces zones. Cette approche simplifie la gestion de la sécurité, renforce la cohérence des politiques et améliore la sécurité globale du réseau.

B. Configuration du workflow de la politique de pare-feu

Une politique de pare-feu solide est essentielle pour protéger les actifs critiques contre les menaces. Comme illustré dans la figure 5, cet article explore les étapes clés de configuration d'une politique de pare-feu performante, offrant aux organisations les outils nécessaires pour contrôler et sécuriser leur trafic réseau de manière proactive.

1) ***Définition des zones****:* Il est nécessaire de définir une zone source et une zone de destination en utilisant l'un des types de configuration disponibles.

2) ***Appariement des zones****:* Les associations de zones sont directionnelles, il est donc important d'apparier les zones dans le sens du trafic prévu.

3) ***Créer une politique de sécurité****:* Au sein de cette politique de sécurité, il est nécessaire de définir une politique de pare-feu spécifique, d'établir des règles de trafic en utilisant des groupes d'objets et des class-maps pour faire correspondre le trafic intéressant, de spécifier une action de pare-feu pour le trafic correspondant, et de définir une action de pare-feu par défaut (par exemple, le rejet par défaut). De plus, la politique de pare-feu est appliquée à une paire de zones spécifique, permettant ainsi la définition et l'application de plusieurs politiques de pare-feu à différentes paires de zones au sein de la politique de sécurité.

4) ***Attacher la politique de sécurité à un modèle de périphérique****:* Après avoir créé la politique de sécurité, elle doit être attachée à un modèle de périphérique. Cela garantit que la politique est déployée sur tous les routeurs associés à ce modèle.

En mettant en place un workflow optimal de politique de pare-feu, les organisations peuvent contrôler proactivement et protéger leur trafic réseau, atténuant les menaces potentielles et renforçant la sécurité globale.

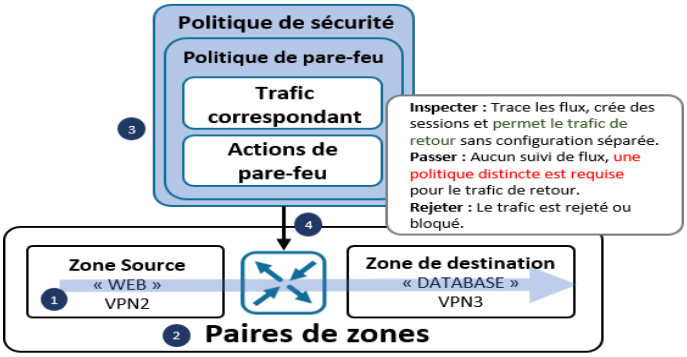


Fig. 5. Workflow de la politique de pare-feu

C. Choix d'actions de pare-feu pour la gestion du trafic

Lors de la configuration des règles de pare-feu, les administrateurs réseau disposent de plusieurs choix d'actions pour gérer le trafic. Ils peuvent inspecter le trafic de manière étatique, le passer en permettant la création de connexions, ou le rejeter pour bloquer les éléments indésirables. En mettant en place une politique de pare-feu performante, les organisations peuvent protéger leur trafic réseau, atténuer les menaces potentielles et renforcer la sécurité globale.

D. Compréhension de la mise en œuvre IDS/IPS dans SD-WAN

Dans les environnements SD-WAN, les systèmes de détection d'intrusions (IDS) et de prévention d'intrusions (IPS) jouent un rôle essentiel dans la protection contre les menaces et attaques connues en temps réel [18]. L'architecture des dispositifs réseau, tels que les routeurs, les pare-feu et autres équipements de sécurité, est primordiale lors de la mise en œuvre des IDS/IPS. Cela nécessite l'utilisation de composants logiciels ou matériels spécialisés capables d'analyser le trafic, de détecter les activités malveillantes et de prendre des mesures proactives pour prévenir ou atténuer les violations de sécurité. Le déploiement d'un moteur IPS approprié, tel que Snort, offre une détection avancée des menaces et des capacités de prévention. Ce moteur IPS peut être déployé dans un environnement adapté, tel qu'un conteneur Linux, pour optimiser les performances en tirant parti de plusieurs cœurs. En combinant une architecture adaptée, un moteur IPS adéquat et des configurations appropriées, les organisations peuvent mettre en place une solide implémentation des IDS/IPS qui renforce la sécurité du réseau et protège contre un large éventail de menaces et d'attaques [19].

E. Amélioration de la sécurité en ligne avec un proxy HTTPS/TLS

L'implémentation d'un proxy HTTPS/TLS joue un rôle fondamental dans les applications basées sur le web qui dépendent d'une communication sécurisée sur Internet. Avec la prédominance du trafic chiffré HTTPS/TLS (Transmission Control Protocol), les dispositifs de sécurité traditionnels sont confrontés à des défis pour appliquer les politiques organisationnelles et détecter les menaces potentielles. Pour relever ces défis, l'utilisation d'un proxy HTTPS/TLS, tel que la fonction de proxy TLS de Cisco SD-WAN, devient indispensable. Comme illustré dans la représentation visuelle 6, ce proxy permet au routeur de bordure d'agir comme un intermédiaire transparent entre les clients et les serveurs, effectuant le chiffrement et le déchiffrement.En assumant à la fois le rôle du client et du serveur, le routeur peut envoyer le trafic de l'application non chiffré vers une inspection et une application des politiques, améliorant ainsi la sécurité et permettant une circulation transparente du trafic. Grâce aux actions configurables du proxy, telles que le "déchiffrement", le "blocage" ou la "non-déchiffrement", le routeur peut prendre des décisions sur la gestion des connexions.

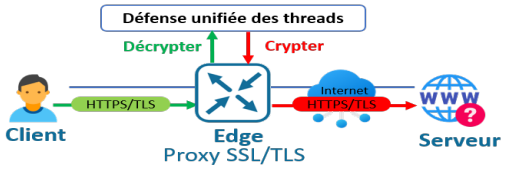


Fig. 6. Le proxy HTTPS/TLS

L'utilisation d'une Autorité de Certification (CA) est également fondamentale dans le processus de proxy TLS, permettant aux proxies TLS de sécuriser l'interception et le déchiffrement du trafic. Il existe quatre options de configuration de CA disponibles dans vManage : CA d'entreprise, CA d'entreprise avec SCEP (Simple Certificate Enrollment Protocol) activé, vManage en tant que CA et vManage en tant que CA intermédiaire. Le choix de la configuration de CA dépend de l'infrastructure à clés publiques PKI (Public Key Infrastructure) de l'organisation.

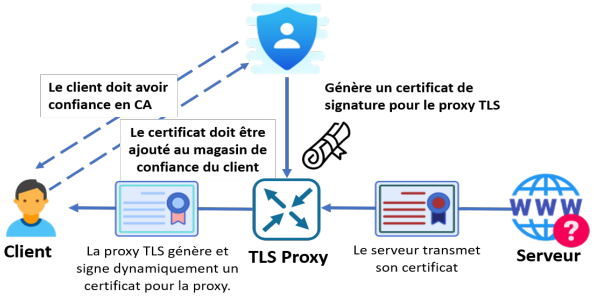


Fig. 7. Proxy TLS et Autorité de Certification (CA)

F. Renforcement de la sécurité Web et du contrôle avec le filtrage d'URL

Les entreprises contemporaines considèrent la sécurité Web comme une priorité majeure dans un paysage en constante évolution. Elles adoptent des solutions robustes telles que

le filtrage d'URL (URLF) pour protéger de manière solide et fiable leurs réseaux contre les menaces potentielles [20]. L'URLF surveille et contrôle le trafic HTTP/HTTPS en inspectant les URL. Lorsqu'un utilisateur envoie une requête HTTP(s) vers un site Web, le système la redirige vers le moteur URLF pour un examen approfondi. Le moteur suit un processus séquentiel basé sur l'URL demandée afin de garantir un filtrage de qualité (voir Figure 8).

Initialement, le moteur vérifie si l'URL est incluse dans la liste blanche définie par l'utilisateur. Si c'est le cas, la requête est autorisée sans autre inspection. À l'inverse, si l'URL est trouvée dans la liste noire, le système répond en présentant une page de blocage ou en redirigeant l'utilisateur pour empêcher l'accès à un contenu potentiellement malveillant.

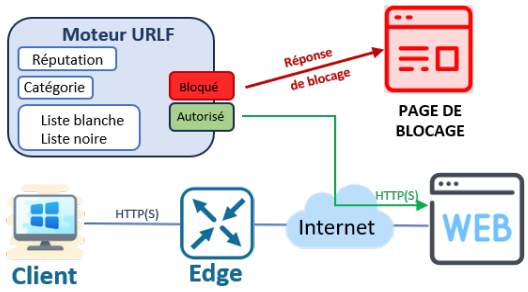


Fig. 8. Aperçu du filtrage d'URL (URLF)

Pour les URL qui ne correspondent ni à la liste blanche ni à la liste noire, le moteur URLF les classe dans l'une des catégories Web prédéfinies. Si la catégorie est autorisée, l'accès est accordé ; sinon, la requête est redirigée vers une page bloquée. De plus, le moteur évalue la réputation Web des sites demandés. Selon le niveau de gravité configuré dans la politique d'URL, l'accès est soit accordé soit redirigé vers une page de blocage.

L'URLF peut utiliser une base de données hébergée localement ou une base de données hébergée dans le cloud. Lors de l'utilisation du cloud, les résultats de recherche sont mis en cache localement pour une récupération instantanée. Les options de filtrage dans l'URLF comprennent les listes d'URL, les catégories Web et la réputation des URL [19]. Les organisations ont la flexibilité d'autoriser ou de refuser les requêtes HTTP(s) en fonction des URL spécifiques, des catégories Web ou des scores de réputation attribués aux sites associés.

G. Protection avancée contre les logiciels malveillants (AMP)

L'AMP est une solution qui renforce la sécurité en analysant en temps réel les téléchargements de fichiers à l'aide des routeurs de bordure. [21]. Voici comment cela fonctionne :

1) ***Interception et Identification de Fichiers****:* Les routeurs de bordure interceptent les téléchargements de fichiers et les envoient au préprocesseur de fichier Snort, qui détecte les potentielles menaces de logiciels malveillants.

2) ***Mise en Cache Locale et Calcul de la Somme de Contrôle****:* Le moteur Snort calcule la somme de contrôle SHA256 du fichier et vérifie si elle est déjà présente dans la mise en cache locale, indiquant si le fichier est connu comme étant propre ou malveillant.

3) ***Exploitation du cloud AMP****:* Si la somme de contrôle ne correspond pas à la mise en cache locale, le fichier est envoyé au cloud AMP pour une analyse plus approfondie. Le cloud AMP utilise une base de données de logiciels malveillants enrichie d'informations contextuelles.

4) ***Attribution d'une Note de Réputation au Fichier****:* Le cloud AMP compare la somme de contrôle SHA256 du fichier avec sa vaste base de données de logiciels malveillants connus et fournit une note de réputation indiquant la probabilité que le fichier soit malveillant.

5) ***Prise de Décision au Niveau du Routeur de Bordure****:* En fonction de la note de réputation attribuée au fichier, le routeur de bordure décide d'autoriser ou de bloquer le téléchargement. Si le fichier est identifié comme propre, le téléchargement se poursuit. S'il est inconnu, le téléchargement est interrompu et le fichier peut être soumis à une analyse supplémentaire.

6) ***Analyse Approfondie avec une Analyse Sécurisée des Logiciels Malveillants****:* Si l'analyse de fichiers est incluse dans la politique de sécurité de l'AMP, le fichier inconnu est transféré vers l'Analyse Sécurisée des Logiciels Malveillants pour une analyse complète dans un environnement de machine virtuelle isolé (sandbox).

7) ***Évaluation globale des menaces et évaluation continue****:* L'Analyse Sécurisée des Logiciels Malveillants attribue une note globale de menace de 1 à 100 au fichier analysé, indiquant la gravité potentielle de la menace. Cette note est renvoyée au cloud AMP pour une prise en charge future.

8) ***Évaluation continue des fichiers****:* Le cloud AMP réévalue en permanence les informations sur les fichiers, même après le téléchargement initial. Cela permet de détecter toute activité malveillante qui pourrait apparaître ultérieurement, mettant à jour la note de menace du fichier pour les futures rencontres.

H. Renforcement de la sécurité réseau avec la protection Web DNS Layer dans Cisco SD-WAN

La sécurité Web DNS Layer est un élément crucial de la stratégie de sécurité du SD-WAN, utilisant le Cloud Umbrella pour prévenir proactivement l'accès à des sites Web malveillants ou inappropriés. En configurant des politiques de sécurité DNS sur le routeur de bordure WAN, les demandes DNS du LAN sont interceptées et redirigées pour évaluation. Le résolveur identifie les sites sécurisés et renvoie leur adresse IP, bloque l'accès aux sites malveillants, ou redirige les demandes vers un proxy intelligent pour une analyse approfondie du contenu. Cette approche renforce la protection en bloquant l'accès aux sites malveillants dès le niveau DNS. [22].

VIII. Sécurité Cloud

La sécurité cloud offre aux entreprises la possibilité de déployer et de gérer leurs applications et données sur des

serveurs distants hébergés sur Internet ou dans le cloud, mais soulève des préoccupations en matière de sécurité. Pour y répondre, les fournisseurs de sécurité cloud SASE proposent des solutions complètes incluant une protection avancée contre les menaces, la sécurité des applications, la protection des données et la sécurité du cloud. Ces solutions intègrent également des services de sécurité tiers tels que la gestion des informations de sécurité et des événements SIEM (Security Information and Event Management), garantissant ainsi une sécurité robuste pour les données et les applications dans l'environnement cloud [23].

IX. Conclusion

L'intégration des technologies SD-WAN et SASE offre des avantages significatifs en termes de connectivité et de sécurité. Grâce à l'infrastructure intelligente de SD-WAN et aux services de sécurité basés sur le cloud de SASE, les organisations peuvent optimiser les performances, réduire les coûts et garantir une protection solide contre les menaces cybernétiques. L'utilisation de Cisco SD-WAN et des fonctionnalités de sécurité de SASE, telles que les pare-feu, les systèmes de prévention des intrusions et la protection contre les logiciels malveillants, contribue à établir une infrastructure réseau sécurisée pour l'ère numérique. La compréhension de ces technologies permet aux organisations de prendre des décisions éclairées lors de la mise en place d'une architecture réseau sécurisée.

References

[1] "From SD-WAN to SASE: How the WAN Evolution is Progressing", Cato Networks. https://www.catonetworks.com/sase/from-sd-wan-to-sase-how-the-wan-evolution-is-progressing/(consulté le 10 Avril 2023).

[2] "5 SD-WAN Best Practices for a Secure and Effective Implementation — Cato Networks. " https://www.catonetworks.com/blog/sd-wan-best-practices-for-secure-and-effective-implementation/ (consulté le 10 Avril 2023).

[3] "SD-WAN Solution - Cisco SD-WAN Solution Overview", Cisco. https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.html(consulté le 11 Avril 2023) .

[4] "SASE Model — Zero Trust Identity". https://network-insight.net/2023/02/03/sase-model-zero-trust-identity/ (consulté le 11 Avril 2023).

[5] "You Can Have It All: SASE and Secure SD-WAN with One SD-Architecture - Cisco Blogs". https://blogs.cisco.com/networking/sase-and-secure-sd-wan-with-one-sd-architecture (consulté le 12 Avril 2023) .

[6] "(PDF) Software-Defined WAN For Dummies · This Software-Defined WAN For Dummies book explains the way for IT and business managers to migrate to a distributed network which is less", dokumen.tips. https://dokumen.tips/documents/softwareadefined-wan-for-dummies-this-softwareadefined-wan-for-dummies-book.html (consulté le 20 Avril 2023) .

[7] P. Segeč, M. Moravčik, J. Uratmová, J. Papán, et O. Yeremenko, "SD-WAN - architecture, functions and benefits", in 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), nov. 2020, p. 593-599. doi: 10.1109/ICETA51985.2020.9379257.

[8] N. Sharma, A. Sharma, et N. Ahlawat, SD-WAN: The Future of Networking. 2023. doi: 10.22214/ijraset.2023.51475.

[9] D. B. Africa, "Guiding Telcos Along the SASE Journey", Digital Business Africa, 8 octobre 2021. https://www.digitalbusiness.africa/en/guiding-telcos-along-the-sase-journey/ (consulté le 20 juin 2023).

[10] "SD-WAN: The Future of Networking". https://www.ijraset.com/research-paper/sd-wan-the-future-of-networking (consulté le 25 Avril 2023).

[11] "Réseau et sécurité, le couple indispensable pour la performance de l'entreprise"a.https://www.journaldunet.com/solutions/dsi/1495429-reseau-et-securite-le-couple-indispensable-pour-la-performance-de-l-entreprise/ (consulté le 25 Avril 2023).

[12] K. Sivakumar, "Cisco Trusted Platforms", Cisco Blogs, 8 avril 2019. https://blogs.cisco.com/sp/cisco-trusted-platforms (consulté le 2 Mai 2023).

[13] "Cisco SD-WAN Controller Certificates and Whitelist Authorization File - Prescr iptive De ploy ment Gu ide - August, 2020". https://www.readkong.com/page/cisco-sd-wan-controller-certificates-and-whitelist-8755520 (consulté le 5 Mai 2023).

[14] "Qu'est-ce que l'IPSec? – Le protocole IPSec expliqué – AWS", Amazon Web Services, Inc. https://aws.amazon.com/fr/what-is/ipsec/ (consulté le 20 Juin 2023).

[15] "Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN — Cisco Press". https://www.ciscopress.com/store/cisco-software-defined-wide-area-networks-designing-9780136533177(consulté le 10 Mai 2023) .

[16] "ePlus-CyberSmart-Awareness-Guide-10-1",

[17] Benjie, "Zone Based Firewall Overview", Study CCNP, 5 février 2022. https://study-ccnp.com/zone-based-firewall-overview/(consulté le 16 Mai 2023) .

[18] "IDS et IPS : en quoi sont-ils différents?" https://www.varonis.com/fr/blog/ids-et-ips-en-quoi-sont-ils-differents (consulté le 20 Mai 2023).

[19] "Security Configuration Guide: Unified Threat Defense, Cisco IOS XE 17 - Snort IPS [Cisco IOS XE Amsterdam 17.2.1]", Cisco. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec-data-utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html (consulté le 20 Mai 2023).

[20] "Using URL filtering with SD-WAN — Lumen". https://www.lumen.com/help/en-us/sd-wan-versa/use-cases/using-url-filtering-with-sd-wan.html (consulté le 2 Juin 2023).

[21] "What is Advanced Malware Protection (AMP)? - TEC Communications: TEC Communications". https://tec4it.com/what-is-advanced-malware-protection-amp/ (consulté le 3 Juin 2023).

[22] "SASE breakdown: DNS-layer security - Cisco Umbrella". https://umbrella.cisco.com/blog/sase-breakdown-dns-layer-security (consulté le 4 Juin 2023).

[23] "What Is SASE - Secure Access Service Edge?", Cisco. https://www.cisco.com/c/en/us/products/security/what-is-sase-secure-access-service-edge.html (consulté le 4 Juin 2023) .